Seniorenzentrum Oberes Reusstal
Gotthardstrasse 33
6484 Wassen

SENIORENZENTRUM
OBERES REUSSTAL WASSEN

Technische und organisatorische Sicherheitsrichtlinien für Mitarbeiter/innen

Meldung von Sicherheits- und Datenschutzvorfällen

Bei Vorfällen wie beispielsweise Erhalt eines Auskunftsbegehrens, Erhalt eines verdächtigen eMails oder seltsames Verhalten der IT sind unverzüglich folgende Personen zu unterrichten:

Datenschutz- und Datensicherheitsverantwortliche/r:
Simone Imhof
Telefon: 041 886 86 86
eMail: leitung@seniorenzentrum-wassen.ch

Stellvertretung:

Telefon:
eMail:

1. Geltungsbereich der Richtlinie

Das Datenschutzgesetz gibt spezifische Informations-, Auskunfts- und Sorgfaltspflichten für Unternehmen vor, welche personenbezogene Daten verarbeiten. Diese Pflichten gewährleisten die Rechte von natürlichen Personen, welche ihre Daten von den Unternehmen verarbeiten lassen. Zu den Sorgfaltspflichten gehören die Gewährleistung der Datensicherheit, damit Daten nicht unberechtigten Dritten zugänglich gemacht werden können.

Sowohl die Institution als auch das Personal unterstehen dem Datenschutzgesetz und sind somit verantwortlich für die Sicherheit der Daten. Die Einhaltung untenstehender Richtlinien ist somit für alle verbindlich.

2. Richtlinie

2.1. Datenaustausch

- Die Weitergabe von Informationen über Bewohnende und Mitarbeitende an Dritte/Angehörige ist grundsätzlich nicht zulässig. Ebenfalls untersagt ist die Weitergabe von betrieblichen Informationen, wie interne Sicherheitsvorkehrungen, Informationen zur IT-Infrastruktur oder Berichtswege. Diese Vorgabe zielt auf die Gefahr des Social Engineerings ab, womit versucht wird, das Vertrauen eines autorisierten Nutzers zu gewinnen und diesen dazu zu verleiten, ihm vertrauliche Informationen über die Netzwerk-Sicherheit zu geben.

- Besonders schützenswerte Daten (Gesundheit, Religion, Strafregister, Gewerkschaft, etc.) dürfen ausschliesslich über HIN oder über adäquate Verschlüsselungsdienste an Dritte gesendet werden. Kein Versenden an Empfängeradressen von @gmail.com, @yahoo.com etc. Damit erfolgt ein Datentransfer nach Amerika als unsicheres Drittland.

- Bei Datenübermittlung auf Internetportalen ist darauf zu achten, dass die Übertragung verschlüsselt ist (Schlösschen in der Adresszeile/https).

- Der Austausch via Fax erfolgt unverschlüsselt und sollte auf ein Minimum beschränkt werden. Fax-Geräte sind so zu positionieren, dass eingehende Nachrichten nicht von unberechtigten Personen eingesehen werden können.

2.2. Incidents

- Datenschutzvorfälle müssen unverzüglich dem Vorgesetzten gemeldet werden. Beispiele für Sicherheitsvorfälle:
  - Auskunftsbegehren durch einen Kunden, Klienten, Mitarbeiter
  - Sicherheitswarnungen der Virenschutzsoftware
  - Verdacht auf Datenverlust, Hackerangriff

  Bitte melden Sie unverzüglich Vorkommnisse, die Ihren Verdacht erregen.

2.3. Organisatorisches

- Das Verwenden des betrieblichen eMail-Accounts zu privaten Zwecken ist untersagt. Für private Korrespondenz bitten wir Sie, einen privaten Webmail Account zu verwenden. Über diesen dürfen selbstverständlich ebenfalls nur private und keine internen Informationen versendet werden.

- Es sind ausschliesslich betriebliche IT-Mittel zu benutzen. Die Verwendung privater Geräte ist untersagt. Das Installieren von privater Software/Apps auf den internen Systemen ist ebenfalls strikt untersagt.

- Private Endgeräte dürfen nicht an das interne Netzwerk angeschlossen werden.

- Nutzung des Internets am Arbeitsplatz:
  Variante1: Die Nutzung des Internets am Arbeitsplatz zu privaten Zwecken ist untersagt.

Variante2: Das private Surfen über den betrieblichen Internetzugang wird toleriert. Wir weisen jedoch darauf hin, dass dieser zu Sicherheitszwecken protokolliert wird.

2.4. Schutz vor Schadsoftware

- Die Nutzung von USB-Sticks ist grundsätzlich untersagt. Ausnahmen müssen mit dem Vorgesetzten abgestimmt werden. Daten auf USB-Sticks können Schadsoftware auf die Arbeitsgeräte und das interne Netzwerk übertragen. Auch aktuelle Virenscanner bieten hiervor keinen 100-prozentigen Schutz. Der einzig sichere Weg, um dieses Risiko zu minimieren, ist der Verzicht auf die Verwendung von USB-Sticks.

- eMail-Nachrichten werden von Cyber Kriminellen häufig verwendet, um unberechtigt an Daten von Unternehmen zu gelangen und Schadsoftware zu verbreiten. Die Absender arbeiten dazu mit verschiedenen Tricks, um dem Empfänger vorzugaukeln ein vertrauenswürdiger und bekannter Geschäftspartner zu sein. Diese Methode ist unter dem Stichwort „Phishing“ bekannt. Wir möchten Sie bitten an diesem Phishing Quiz teilzunehmen, damit Sie Ihre Kenntnisse zu diesem Thema testen können. https://phishingquiz.withgoogle.com. Zu Beginn werden Sie nach Ihrem Namen und Ihrer eMailadresse gefragt. Diese Daten werden nur zu Demonstrationszwecken gebraucht. Wir bitten Sie nur Demodaten einzugeben wie beispielsweise Max Mustermann / test@test.ch.
  Sollte Ihnen im Umgang mit eMails etwas seltsam vorkommen oder Sie sind nicht sicher, ob Sie versehentlich ein kritisches eMail angeklickt haben, melden Sie dies bitte umgehend der Sicherheitsverantwortlichen.

- Bei allfälligen Meldungen der Virensoftware ist der Vorgesetzte unverzüglich zu kontaktieren. Am Rechner sind keine Handlungen mehr zu vollziehen.

- Endgeräte dürfen nicht für private Zwecke verwendet werden.

2.5. Zugriffsschutz

- Der Bildschirm muss bei jedem Verlassen des Arbeitsplatzes gesperrt werden (Tastenkombination Windows-Taste + L). Zum erneuten Zugriff ist die Eingabe des Kennwortes erforderlich. Diese Massnahme schützt Ihren PC vor unberechtigtem Zugriff während Ihrer Abwesenheit.

- Bei ausser Betrieb genommenen IT-Mitteln, insbesondere bei Endgeräten, sind alle Daten unmittelbar nach der Ausserbetriebnahme und vor der Entsorgung vollständig und unwiderruflich zu löschen.

- Starke Passwörter schützen unsere IT vor unberechtigtem Zugriff. Unsere Passwort Policy fordert mindestens 8 Zeichen, enthalten Grossbuchstaben, Kleinbuchstaben, Zahlen und Sonderzeichen. Es dürfen keine Begriffe verwendet werden, die auch in einem Wörterbuch stehen. Trotzdem gut zu merken sind Passwörter die beispielsweise aus den Anfangsbuchstaben eines Satzes bestehen. Beispiel: Ich bin Fan von Musik aus den 80igern! IbFvMad8! Das physische Hinterlegen von Passwörtern (z. B. Post-IT unter der Tastatur) ist untersagt.

- Der Zutritt zu den Räumlichkeiten und zu den IT-Systemen ist gegen Unbefugte zu schützen. Betriebsfremde Personen dürfen sich nicht unbeaufsichtigt in den internen Räumlichkeiten aufhalten. Dies dient als Schutz davor, dass unberechtigte Personen Zugang zu internen und/oder besonders schützenswerten Daten erhalten.

- Sämtliche gedruckten Unterlagen, welche personenbezogene oder interne Informationen enthalten, müssen geschreddert werden. Diese dürfen keinesfalls im Altpapier entsorgt werden.